Приложение
к распоряжению администрации
города Мурманска
от 11.04.2023 № 18-р

Регламент подключения участников к защищённой виртуальной сети администрации города Мурманска и организации межсетевого взаимодействия

Термины и определения, используемые в настоящем регламенте подключения участников к защищённой виртуальной сети администрации города Мурманска и организации межсетевого взаимодействия (далее – Регламент):

– ViPNet Administrator – программное обеспечение, предназначенное для конфигурирования и управления виртуальной защищенной сетью, организованной с использованием технологии ViPNet;

– ViPNet Client – программное обеспечение, реализующее на рабочем месте пользователя функции VPN-клиента, персонального экрана и клиента защищенной почтовой службы;

– ViPNet Coordinator – программно-аппаратный комплекс, выполняющий функцию узла виртуальной защищенной сети, организованной с использованием технологии ViPNet;

– VPN (Virtual Private Network) – обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети;

– Абонентский пункт – персональный компьютер с установленным программным обеспечением ViPNet Client, входящий в состав защищенной виртуальной сети администрации города Мурманска;

– АГМ – администрация города Мурманска;

– Администратор безопасности Участника ЗВС АГМ (Администратор безопасности Участника) – муниципальный служащий (сотрудник) юридического лица, подключенного к защищенной виртуальной сети администрации города Мурманска в установленном в настоящем Регламенте порядке, ответственный за поэкземплярный учет и контроль эксплуатации сетевых узлов защищенной виртуальной сети администрации города Мурманска со стороны своей организации и установку средств криптографический защиты информации в своей организации;

– Администратор ЗВС АГМ – юридическое лицо, на которое возложены функции организационно-технического сопровождения работы защищенной виртуальной сети администрации города Мурманска и ее развития, координации действий юридических лиц, подключенных к защищенной виртуальной сети администрации города Мурманска в установленном в настоящем Регламенте порядке, заключившее соответствующий договор с администрацией города

Мурманска и обладающее необходимой разрешительной (лицензионной) базой в соответствии с действующим законодательством;

– Владелец ЗВС АГМ – структурное подразделение администрации города Мурманска, осуществляющее координацию действий юридических лиц, подключенных к защищенной виртуальной сети администрации города Мурманска в установленном в настоящем Регламенте порядке, разработку организационно-распорядительных документов, регламентирующих работу в защищенной виртуальной сети администрации города Мурманска, подготовительные работы по организации предоставления доступа к компонентам защищенной виртуальной сети администрации города Мурманска на основании заявок и соглашений (отдел информационно-технического обеспечения и защиты информации администрации города Мурманска);

– дистрибутив ключей – файл с расширением .dst, создаваемый в программном обеспечении ViPNet Administrator для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программного обеспечения ViPNet на сетевом узле;

– доверенный способ передачи информации – способ передачи информации, обеспечивающий требуемые уровни безопасности и конфиденциальности;

– защищенная виртуальная сеть администрации города Мурманска (ЗВС АГМ) – защищенная виртуальная транспортная сеть, наложенная на физические каналы связи, построенная с использованием технологий межсетевого экранирования и VPN, реализованная сертифицированными в установленном порядке средствами защиты информации;

– информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

– компрометация защищаемой (ключевой) информации – факт доступа (подозрение на факт доступа) посторонних лиц к защищаемой (ключевой) информации;

– Компонент ЗВС АГМ (Компонент) – сетевой узел, обеспечивающий функционирование защищенной виртуальной сети администрации города Мурманска и представляющий собой программное обеспечение, программно-аппаратный комплекс ViPNet;

– контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных, технических и иных материальных средств;

– несанкционированный доступ – доступ к закрытой (ограниченной в законном порядке) информации посторонних лиц, не имеющих разрешения на доступ к такой информации;

– оператор информационной системы – юридическое лицо, осуществляющее деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

– Пользователь Участника ЗВС АГМ (Пользователь Участника) – муниципальный служащий (сотрудник) юридического лица, подключенного к защищенной виртуальной сети администрации города Мурманска в установленном в настоящем Регламенте порядке, использующий для выполнения своих служебных обязанностей и доступа к информационным системам и ресурсам посредством защищенной виртуальной сети администрации города Мурманска персональный компьютер с установленным программным обеспечением ViPNet Client или персональный компьютер, находящийся в сегменте сети Участника, подключенном к защищенной виртуальной сети администрации города Мурманска посредством программно-аппаратного комплекса ViPNet Coordinator с использованием технологии туннелирования;

– Претендент – юридическое лицо (структурные подразделения АГМ, подведомственные им учреждения, иные организации), имеющее намерение подключиться к защищенной виртуальной сети администрации города Мурманска;

– резервный набор персональных ключей пользователя – набор, предназначенный для обновления ключевой информации в случае смены мастер-ключа персональных ключей или в случае перехода на новый вариант персонального ключа пользователя;

– технология ViPNet – технология, предназначенная для построения виртуальных защищенных сетей путем использования системы персональных и межсетевых экранов на защищаемых компонентах распределенной сети и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающие шифрование сетевого трафика между этими элементами;

– туннелирование – технология ViPNet, позволяющая защитить соединения между узлами локальных сетей, которые обмениваются информацией через сеть Интернет или другие публичные сети, путем инкапсуляции и шифрования трафика этих узлов не самими узлами, а координаторами, которые установлены на границе их локальных сетей. При этом установка программного обеспечения ViPNet Client на эти узлы необязательна. Туннелируемые узлы могут быть как защищенными, так и открытыми;

– Участник ЗВС АГМ (Участник) – юридическое лицо (структурные подразделения администрации города Мурманска, подведомственные им учреждения, иные организации), являющееся пользователем информационных систем, доступ к которым осуществляется посредством защищенной виртуальной сети администрации города Мурманска; юридические и физические лица, осуществляющие обслуживание информационных систем и ресурсов юридических лиц, осуществляющих деятельность по эксплуатации информационных систем, на договорной основе и подключенные к защищенной

виртуальной сети администрации города Мурманска в установленном в настоящем Регламенте порядке;

– центр управления сетью – аппаратные и/или программные средства для мониторинга, конфигурирования и управления компонентами защищенной виртуальной сети администрации города Мурманска.

1. Общие положения

1.1. Настоящий Регламент разработан в соответствии со следующими нормативно-правовыми актами Российской Федерации:

– Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– приказом ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

– приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– приказом ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

– иными нормативно-правовыми и подзаконными актами Российской Федерации, рекомендательными документами государственных регуляторов в области защиты информации и информационной безопасности.

1.2. Настоящий Регламент определяет и устанавливает:

1.2.1. Назначение ЗВС АГМ.

1.2.2. Организацию обслуживания и работы ЗВС АГМ.

1.2.3. Структуру и состав ЗВС АГМ.

1.2.4. Порядок подключения Участников к ЗВС АГМ. Отключение от ЗВС АГМ.

1.2.5. Порядок изменения направлений связи и/или предоставления доступа к информационным системам или ресурсам.

1.2.6. Организацию межсетевого взаимодействия с другими защищенными сетями.

1.2.7. Порядок действий при компрометации защищаемой (ключевой) информации.

1.2.8. Технические мероприятия.

1.2.9. Порядок разрешения конфликтных ситуаций.

1.2.10. Внесение изменений (дополнений) в настоящий Регламент.

1.3. ЗВС АГМ реализована с использованием программно-аппаратных комплексов и программного обеспечения, основанного на технологии ViPNet.

1.4. В настоящий Регламент могут быть внесены изменения, связанные с развитием (изменением) технологии обработки информации на Компонентах ЗВС АГМ, изменением структуры ЗВС АГМ, а также изменениями в действующем законодательстве РФ в области информационной безопасности и технической защиты информации (в том числе криптографическими методами). Предложения по внесению изменений в настоящий Регламент направляются Администратором ЗВС АГМ, Участниками ЗВС АГМ Владельцу ЗВС АГМ.

2. Назначение ЗВС АГМ

2.1. Целью создания ЗВС АГМ является обеспечение информационной безопасности при передаче информации между Участниками ЗВС АГМ, в том числе информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, с использованием публичных и выделенных каналов связи путем организации виртуальной сети.

2.2. ЗВС АГМ обеспечивает выполнение следующих задач:

2.2.1. Предотвращение несанкционированного доступа к информации, в том числе информации ограниченного доступа, и (или) передачи ее лицам, не имеющим права на доступ к информации.

2.2.2. Защиту конфиденциальной информации, иной охраняемой законодательством Российской Федерации информации, в том числе персональных данных, при взаимодействии информационных систем или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями.

2.2.3. Организацию защищенного информационного взаимодействия между Участниками, в том числе в целях реализации Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

2.3. ЗВС АГМ создана на основе информационно-вычислительной сети АГМ (далее – ИВС АГМ), включающей в себя локальную вычислительную сеть здания АГМ, являющуюся узловым (центральным) компонентом системы, и подключенные к ней локальные вычислительные сети иных зданий. Объединение в единую ИВС АГМ осуществляется с использованием выделенных каналов передачи данных.

3. Организация обслуживания и работы ЗВС АГМ

3.1. Администратор ЗВС АГМ.

3.1.1. Администратор ЗВС АГМ выполняет следующие функции:

– обеспечивает администрирование ЗВС АГМ, наблюдение за работоспособностью защищенной сети и принимает меры по восстановлению ее работоспособности;

– осуществляет установку и настройку компонентов ЗВС АГМ в сегменте Участника по согласованию с Участником;

– осуществляет подключение к ЗВС АГМ новых Участников в соответствии с заявками на подключение, согласованными Владельцем ЗВС АГМ;

– осуществляет профилактические работы Компонентов ЗВС АГМ и техническое сопровождение ЗВС АГМ.

3.1.2. Обязанности Администратора ЗВС АГМ:

– осуществление поддержки работоспособности компонентов ЗВС АГМ;

– предоставление Владельцу ЗВС АГМ информации о состоянии компонентов ЗВС АГМ, в том числе о требующих замены или модернизации;

– информирование Администраторов безопасности Участников о проводимых работах по обслуживанию и возможных перебоях в работе ЗВС АГМ;

– соблюдение конфиденциальности информации, полученной в связи с выполнением своих обязанностей.

3.1.3. Администратор ЗВС АГМ несет ответственность за невыполнение требований настоящего Регламента, а также требований технической и эксплуатационной документации на Компоненты ЗВС АГМ и нормативно-правовых актов, регулирующих работу ЗВС АГМ, нормативно-правовых актов в области защиты информации.

3.2. Владелец ЗВС АГМ.

3.2.1. Владелец ЗВС АГМ выполняет следующие функции:

– рассматривает заявления Участников на подключение к ЗВС АГМ;

– осуществляет на основании согласованных заявлений и соглашений подготовительные работы по организации предоставления доступа к компонентам ЗВС АГМ и передает информацию о необходимости подключения Участника Администратору ЗВС АГМ;

– формирует и поддерживает в актуальном состоянии электронный реестр Участников, подключенных к ЗВС АГМ;

– разрабатывает, вводит в действие и предоставляет Участникам организационно-распорядительные документы, регламентирующие порядок и условия подключения к ЗВС АГМ, порядок работы Участников в ЗВС АГМ, проекты заявлений и соглашений о подключении к ЗВС АГМ;

– рассматривает предложения по формированию и внедрению Компонентов ЗВС АГМ, поступивших от Администратора ЗВС АГМ, Участников ЗВС АГМ;

– осуществляет мероприятия по модернизации и развитию ЗВС АГМ.

3.2.2. Права Владельца ЗВС АГМ:

– запрашивать у Администратора ЗВС АГМ информацию о компонентах ЗВС АГМ;

– запрашивать и получать от Участников необходимые материалы и сведения об использовании ими ЗВС АГМ;

– разрабатывать документацию по вопросам, касающимся эксплуатации и

управления ЗВС АГМ;

– проводить проверки Участников ЗВС АГМ на предмет исполнения требований настоящего Регламента и действующего законодательства в области защиты информации пользователями Участников ЗВС АГМ и принимать решение об отключении или ограничении доступа к ЗВС АГМ в случаях обнаружения нарушений.

3.2.3. Владелец ЗВС АГМ несет ответственность за невыполнение требований настоящего Регламента, а также требований технической и эксплуатационной документации на Компоненты ЗВС АГМ, установленные непосредственно в АГМ, и нормативно-правовых актов, регулирующих работу ЗВС АГМ, нормативно-правовых актов в области защиты информации.

3.3. Администратором безопасности Участника ЗВС АГМ назначается муниципальный служащий (сотрудник) Участника. В случае смены лица, на которого возложены функции Администратора безопасности Участника, Участник обязан в течение пяти рабочих дней известить об этом Владельца ЗВС АГМ и Администратора ЗВС АГМ в письменной форме. Зоной ответственности Администратора безопасности Участника является локальная вычислительная сеть, в которой расположены и подключены Компоненты ЗВС АГМ, пользователям которой предоставляется доступ к информационным системам или ресурсам посредством ЗВС АГМ.

3.3.1. Обязанности Администратора безопасности Участника:

– контроль эксплуатации Компонентов ЗВС АГМ, установленных у Участника;

– контроль соблюдения Пользователями Участника конфиденциальности при обращении со сведениями, которые им доверены или стали известны в процессе работы в ЗВС АГМ о функционировании и порядке обеспечения безопасности применяемых Компонентов ЗВС АГМ и ключевых документов к ним;

– ознакомление Пользователей Участника с правилами работы со средствами криптографической защиты информации (далее – СКЗИ), требованиями безопасности и ответственности за нарушение действующего законодательства в области защиты информации;

– эксплуатация и хранение СКЗИ, технической и эксплуатационной документации, ключевых документов, носителей информации ограниченного распространения, относящихся к Компонентам ЗВС АГМ в соответствии с требованиями действующего законодательства;

– уведомление руководителя Участника, Администратора ЗВС АГМ и Владельца ЗВС АГМ о действиях пользователей, осуществивших несанкционированный доступ к информационным системам или ресурсам, доступ к которым осуществляется посредством ЗВС АГМ, или нарушивших другие требования по обеспечению безопасности информации.

3.3.2. Администратор безопасности Участника несет ответственность:

– за невыполнение требований настоящего Регламента, а также требований технической и эксплуатационной документации на компоненты ЗВС

АГМ и нормативно-правовых актов, регулирующих работу ЗВС АГМ, нормативно-правовых актов в области защиты информации;

– за соблюдение конфиденциальности информации, полученной в связи с выполнением своих обязанностей.

3.4. Пользователи Участника.

3.4.1. Пользователь Участника обязан:

– знать и соблюдать правила информационной безопасности при работе с СКЗИ, требования настоящего Регламента, а также других актов, регулирующих работу ЗВС АГМ;

– соблюдать конфиденциальность информации, полученной в связи с выполнением своих обязанностей;

– при работе в ЗВС АГМ выполнять только задания, связанные с должностными обязанностями;

– при выявлении вредоносных программ или признаков нештатного функционирования программного обеспечения немедленно сообщить о данном инциденте Администратору безопасности Участника, Администратору ЗВС АГМ и Владельцу ЗВС АГМ;

– обеспечивать безопасность хранения ключевой информации и (или) пароля.

3.4.2. Пользователю Участника запрещается:

– оставлять свой Абонентский пункт либо персональный компьютер, находящийся в сегменте сети Участника, подключенном к ЗВС АГМ, во включенном состоянии без контроля и с незаблокированными устройствами ввода и отображения информации;

– допускать к подключенному в ЗВС АГМ Абонентскому пункту или рабочей станции посторонних лиц;

– самостоятельно проводить изменения в настройках Абонентского пункта;

– передавать пароли и ключевую информацию третьим лицам, а также размещать их в местах, доступных посторонним.

3.4.3. Пользователи Участника несут ответственность за невыполнение требований настоящего Регламента, а также требований технической и эксплуатационной документации на Компоненты ЗВС АГМ и нормативно-правовых актов, регулирующих работу ЗВС АГМ, нормативно-правовых актов в области защиты информации.

4. Структура и состав ЗВС АГМ

4.1. ЗВС АГМ представляет собой территориально распределенную информационно-телекоммуникационную сеть, объединяющую Компоненты ЗВС АГМ.

4.2. Предоставление доступа Участника к информационным системам или ресурсам, размещенным на оборудовании, входящем в состав ИВС АГМ, осуществляется с использованием Компонентов ЗВС АГМ.

4.3. Взаимодействие Компонентов ЗВС АГМ осуществляется по каналам связи, используемым Участниками.

4.4. Компоненты, обеспечивающие функционирование ЗВС АГМ, включают в себя ViPNet Administrator, ViPNet Coordinator, а также ViPNet Client, устанавливаемый на оборудовании Участников.

4.5. Участник обязан обеспечить информационную безопасность и техническую защиту информации каждого подключаемого Компонента в соответствии с законодательством Российской Федерации, а также технической и эксплуатационной документацией на Компоненты.

4.6. Компоненты, устанавливаемые у Участников:

– должны находиться в пределах контролируемой зоны Участников, быть в работоспособном состоянии, доступными для других Участников при защищенном и межсетевом взаимодействии, за исключением времени проведения ремонтных и планово-профилактических работ, осуществляемых Администратором ЗВС АГМ;

– должны иметь действующие сертификаты соответствия средств защиты информации по требованиям безопасности информации и быть введены в эксплуатацию в соответствии с технической и эксплуатационной документацией на Компоненты.

5. Порядок подключения участников к ЗВС АГМ. Отключение от ЗВС АГМ

5.1. Организация подключения новых Участников включает в себя следующие этапы:

5.1.1. Подача Претендентом комплекта документов на подключение к ЗВС АГМ.

5.1.2. Рассмотрение комплекта документов Владельцем ЗВС АГМ, информирование Претендента о результатах рассмотрения.

5.1.3. Приобретение Участником в случае необходимости соответствующего программного обеспечения.

5.1.4. Подключение Участника к ЗВС АГМ посредством Компонента ViPNet Client.

5.1.5. Подключение Участника к ЗВС АГМ посредством Компонента в исполнении программно-аппаратного комплекса ViPNet Coordinator.

5.2. Подача Претендентом комплекта документов на подключение к ЗВС АГМ.

5.2.1. Претендент формирует и направляет Владельцу ЗВС АГМ комплект документов о намерении подключиться к ЗВС АГМ с указанием цели подключения, количестве Абонентских пунктов (в случае организации подключения Пользователей Участника посредством Компонента ViPNet Client), перечня информационных систем или ресурсов, с которыми необходима организация защищённого информационного обмена.

5.2.2. В комплект документов, передаваемый Претендентом, входят:

– заявление на подключение к ЗВС АГМ, оформленное в соответствии с приложением № 1 к настоящему Регламенту, в двух экземплярах;

– заявление на регистрацию пользователя ЗВС АГМ, оформленное в соответствии с приложением № 2 к настоящему Регламенту, в двух экземплярах в случае организации подключения Пользователей Участника посредством Компонента ViPNet Client.

В случае организации физического подключения сегмента локальной сети Участника с использованием технологии туннелирования посредством Компонента в исполнении программно-аппаратного комплекса ViPNet Coordinator, установленного в контролируемой зоне одного из Участников, направляется только заявление на подключение к ЗВС АГМ.

5.3. Рассмотрение комплекта документов Владельцем ЗВС АГМ, информирование Претендента о результатах рассмотрения.

5.3.1. Владелец ЗВС АГМ в течение семи рабочих дней со дня получения комплекта документов проводит оценку оснований для подключения Претендента к ЗВС АГМ, технической возможности организации связей и доступа к информационным системам или ресурсам, указанным в заявлении. При необходимости проведения процедуры согласования комплекта документов Претендента с Оператором информационной системы время рассмотрения комплекта документов может быть увеличено.

5.3.2. Приобретение программного обеспечения до даты рассмотрения комплекта документов о намерении подключиться к ЗВС АГМ не является основанием и гарантией подключения Претендента.

5.3.3. Решение о подключении к ЗВС АГМ направляется в электронной форме в адрес Претендента, указанный в заявлении на подключение. При положительном решении Претендент становится Участником. Вторые экземпляры согласованных Владельцем ЗВС АГМ заявлений возвращаются Участнику с целью последующей передачи Администратору ЗВС АГМ для осуществления подключения Участника.

5.3.4. В случае отрицательного результата рассмотрения комплекта документов Владелец ЗВС АГМ уведомляет Претендента об отказе в подключении к ЗВС АГМ. Решение об отказе направляется в электронной форме в адрес Претендента, указанный в заявлении на подключение.

5.4. Приобретение Участником в случае необходимости соответствующего программного обеспечения.

5.4.1. Подключение Участника осуществляется с использованием Компонента ViPNet Client или физического подключения сегмента локальной сети Участника с использованием технологии туннелирования посредством Компонента в исполнении программно-аппаратного комплекса ViPNet Coordinator. В случае подключения Участника с использованием Компонента ViPNet Client необходимо приобретение лицензий на данное программное обеспечение. Количество необходимых для подключения лицензий приобретается Участником самостоятельно. При оформлении документов на приобретение лицензии на программное обеспечение новый Участник указывает регистрационный номер сети ViPNet – 4195. Количество приобретаемых

лицензий должно соответствовать количеству планируемых к подключению рабочих станций нового Участника, указанных в заявительных документах. В случае подключения Участника посредством физического подключения сегмента локальной сети Участника с использованием технологии туннелирования посредством Компонента в исполнении программно-аппаратного комплекса ViPNet Coordinator приобретение лицензий ViPNet Client не требуется, если такое требование не установлено порядком доступа к подключаемым информационным системам Оператора.

5.4.2. Подключение Участника к ЗВС АГМ с использованием Компонента ViPNet Client осуществляется Администратором ЗВС АГМ в течение трех рабочих дней с даты получения регистрационных файлов (файлов, содержащих информацию о приобретенных Участником лицензиях) от производителя программного обеспечения или представителя производителя программного обеспечения ViPNet.

5.5. Подключение Участника к ЗВС АГМ посредством Компонента ViPNet Client.

5.5.1. Участник для получения дистрибутива ключевой информации и пароля доступа к нему должен направить к Администратору ЗВС АГМ Администратора безопасности Участника/Пользователя Участника/иного представителя Участника с согласованными Владельцем ЗВС АГМ экземплярами заявлений и доверенностью представителя Участника, оформленной в соответствии с приложением № 3 к настоящему Регламенту.

5.5.2. Факт выдачи дистрибутива ключевой информации заносится в Журнал поэкземплярного учета ключевых документов Администратора ЗВС АГМ. В обязательном порядке для Администратора безопасности Участника/Пользователя Участника или иного представителя Участника проводится краткий инструктаж по обращению с СКЗИ с фиксированием факта проведения инструктажа в журнале установленной формы, а также осуществляется выдача порядка действий при компрометации ключевой информации.

5.5.3. Повторное формирование дистрибутива ключевой информации зарегистрированного Абонентского пункта, в том числе в случаях внесения в ЗВС АГМ изменений, инициированных Администратором ЗВС АГМ, повлекших за собой неработоспособность Абонентского пункта Участника, производится на основании подачи Участником заявления, оформленного в соответствии с приложением № 4 к настоящему Регламенту.

5.5.3.1. Формирование дистрибутива ключевой информации осуществляется Администратором ЗВС АГМ в течение трех рабочих дней с даты получения от Участника соответствующего заявления. По завершении обозначенных работ Администратор ЗВС АГМ уведомляет об этом Участника в электронной форме на адрес, указанный в заявлении.

5.5.3.2. Получение дистрибутива ключевой информации производится Участником в соответствии с подпунктами 5.5.1 и 5.5.2 настоящего Регламента.

5.5.4. Формирование дистрибутива ключевой информации дополнительных Абонентских пунктов уже подключенного Участника

производится на основании подачи Участником дополнительных заявлений в двух экземплярах, оформленных в соответствии с приложением № 2 к настоящему Регламенту и согласованных Владельцем ЗВС АГМ.

5.5.4.1. Формирование дистрибутива ключевой информации осуществляется Администратором ЗВС АГМ в течение трех рабочих дней с даты получения от Участника соответствующего второго экземпляра заявления. По завершении обозначенных работ Администратор ЗВС АГМ уведомляет об этом Участника в электронной форме на адрес, указанный в заявлении.

5.5.4.2. Получение дистрибутива ключевой информации производится Участником в соответствии с подпунктами 5.5.1 и 5.5.2 настоящего Регламента.

5.6. Подключение Участника к ЗВС АГМ посредством Компонента в исполнении программно-аппаратного комплекса ViPNet Coordinator.

5.6.1. В случае принятия Владельцем ЗВС АГМ решения о возможности подключения Участника к ЗВС АГМ посредством программно-аппаратного комплекса ViPNet, установленного в пределах контролируемой зоны одного из Участников, Администратор ЗВС АГМ при участии Администратора безопасности Участника на основании согласованного Владельцем ЗВС АГМ заявления на подключение осуществляет подключение сегмента локальной вычислительной сети Участника к программно-аппаратному комплексу ViPNet Coordinator.

5.6.2. Программно-аппаратный комплекс ViPNet Coordinator может быть установлен как в границах контролируемой зоны непосредственно подключаемого Участника, так и в контролируемой зоне Участника, уже подключенного к ЗВС АГМ при условии, что Участники находятся в пределах одного здания.

5.7. Участник имеет право произвести отключение от ЗВС АГМ, направив Владельцу ЗВС АГМ соответствующее заявление, оформленное в соответствии с приложением № 7 к настоящему Регламенту.

Отключение Участника от ЗВС АГМ осуществляется Администратором ЗВС АГМ в течение двух рабочих дней с даты получения от Владельца ЗВС АГМ соответствующего заявления Участника.

5.8. На Участника распространяются все обязанности по соблюдению требований информационной безопасности, установленных действующим законодательством в области защиты информации, технической и эксплуатационной документацией на Компоненты и настоящим Регламентом.

6. Порядок изменения направлений связи и/или предоставления доступа к информационным системам или ресурсам

6.1. Участник, желающий изменить направление связей и/или получить доступ к информационным системам или ресурсам посредством ЗВС АГМ, направляет в адрес Владельца ЗВС АГМ заявление в двух экземплярах, оформленное в соответствии с приложением № 5 к настоящему Регламенту.

6.2. Владелец ЗВС АГМ в течение пяти рабочих дней со дня получения рассматривает заявление, проводит оценку технической возможности для

изменения направлений связи и/или организации доступа к информационным системам или ресурсам, указанным в заявлении.

6.3. Владелец ЗВС АГМ имеет право отказать Участнику в изменении направлений связи и/или организации доступа к информационным системам или ресурсам, объяснив причину отказа. Решение об отказе в изменении направлений связи и/или организации доступа к информационным системам или ресурсам направляется в электронной форме в адрес Участника в течение трех рабочих дней со дня принятия указанного решения. В случае принятия положительного решения вторые экземпляры согласованных Владельцем ЗВС АГМ заявлений возвращаются Участнику ЗВС АГМ для последующей передачи Администратору ЗВС АГМ для выполнения.

6.4. В течение трех рабочих дней с даты получения от Участника ЗВС АГМ согласованного Владельцем ЗВС АГМ заявления об изменении направлений связи и/или организации доступа к информационным системам или ресурсам посредством ЗВС АГМ Администратор ЗВС АГМ вносит соответствующие изменения в структуру ЗВС АГМ или правила доступа к информационным системам или ресурсам посредством ЗВС АГМ в соответствии с заявлением и направляет справочную и ключевую информацию на соответствующие Компоненты ЗВС АГМ.

6.5. По завершении обозначенных работ Администратор ЗВС АГМ направляет уведомление в электронной форме в адреса Участника ЗВС АГМ и Владельца ЗВС АГМ.

7. Организация межсетевого взаимодействия с другими защищенными сетями

7.1. Для организации межсетевого взаимодействия (далее – МСВ) между ЗВС АГМ и организацией, подключенной или владеющей сторонней сетью ViPNet (далее – Организация), Организация готовит информационное письмо, в котором информирует Владельца ЗВС АГМ о необходимости организации информационного МСВ с указанием контактов ответственных лиц.

7.2. Владелец ЗВС АГМ совместно с Администратором ЗВС АГМ в течение пяти рабочих дней со дня получения информационного письма проводит оценку оснований и технической возможности для организации МСВ.

7.3. После принятия решения об организации либо об отказе в организации МСВ Владелец ЗВС АГМ в письменной форме либо по электронной почте уведомляет о принятом решении Организацию, инициирующую данное взаимодействие.

7.4. При положительном решении Владелец ЗВС АГМ в течение трех рабочих дней направляет на подписание в организацию, инициирующую данное взаимодействие, соглашение об установлении межсетевого взаимодействия (далее – Соглашение), оформленное в соответствии с приложением № 8 к настоящему Регламенту.

7.5. После подписания Соглашения Администратор ЗВС АГМ и Администратор сторонней сети ViPNet в соответствии с технической и

эксплуатационной документацией на программное обеспечение ViPNet организует МСВ с формированием необходимой справочной и ключевой информации.

7.6. Ключевая и справочная информация, необходимая для организации МСВ (начальный и ответный экспорт), передается между соответствующими защищенными сетями исключительно доверенным способом.

7.7. После завершения процедуры организации МСВ подписывается протокол установления межсетевого взаимодействия, оформленный в соответствии с приложением № 1 к Соглашению (приложение № 8 к настоящему Регламенту).

7.8. В случае инициативы организации МСВ со стороны Владельца ЗВС АГМ в адрес Организации направляется информационное письмо, содержащее информацию о цели подключения и запрос технической возможности организации МСВ.

При положительном решении стороны, организующие МСВ, осуществляют мероприятия в соответствии с регламентом сторонней сети ViPNet и с пунктами 7.6, 7.7 настоящего Регламента.

7.9. При организации МСВ в обязательном порядке выполняются требования по информационной безопасности и технической защите информации, предъявляемые действующим законодательством РФ, а также действующими Регламентами (Положениями) АГМ и Организации.

8. Порядок действий при компрометации защищаемой (ключевой) информации

8.1. К событиям компрометации, когда ключи Абонентского пункта считаются скомпрометированными, относятся следующие случаи:

– посторонним лицам мог стать доступен (стал доступен) файл дистрибутива ключевой информации Абонентского пункта;

– посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на Абонентском пункте;

– увольнение сотрудников, являющихся Пользователями ЗВС АГМ, имевших доступ к ключевой информации, а также иные события, указанные в технической и эксплуатационной документации на Компонент ЗВС АГМ.

8.2. При возникновении возможности (предполагаемой возможности) нарушения конфиденциальности ключевой информации и (или) аутентификационных данных Абонентского пункта, при условии, что доступ к Абонентскому пункту посторонних лиц был возможен, ключевая информация считается скомпрометированной.

8.3. При наступлении любого из перечисленных в пункте 8.1 настоящего Регламента событий Пользователь Участника должен немедленно прекратить работу на Абонентском пункте и сообщить о факте компрометации (или предполагаемом факте компрометации) Администратору безопасности Участника или в случае отсутствия такового напрямую Владельцу ЗВС АГМ и Администратору ЗВС АГМ.

8.4. Администратор безопасности Участника/Пользователь в кратчайшие сроки уведомляет Владельца ЗВС АГМ и Администратора ЗВС АГМ о факте и обстоятельствах компрометации любым доступным способом: по телефону, факсу, электронной почте и т.д.

8.5. Администратор безопасности Участника/Пользователь обязан после уведомления о компрометации (угрозе компрометации) направить в адрес Владельца ЗВС АГМ и Администратора ЗВС АГМ подписанное руководителем Участника и заверенное печатью Участника уведомление о компрометации ключей Абонентского пункта, оформленное в соответствии с приложением № 6 к настоящему Регламенту.

8.6. Администратор ЗВС АГМ при получении сообщения о компрометации ключевой информации обязан в кратчайшие сроки объявить ключевую информацию данного пользователя скомпрометированной и незамедлительно создать справочники связей для компрометации с необходимой информацией.

8.7. Администратор ЗВС АГМ осуществляет формирование новой ключевой информации и рассылку сформированных обновлений ключей на Абонентские пункты, а также оповещает о факте компрометации ключей всех пользователей, связанных со скомпрометированным пользователем.

8.8. Администратор ЗВС АГМ формирует новую ключевую информацию для скомпрометированного Абонентского пункта:

– при наличии на скомпрометированном Абонентском пункте резервного набора персональных ключей пользователя и отсутствия факта компрометации этого набора формирует и высылает новый ключевой набор персональных ключей пользователя;

– в остальных случаях обеспечивает передачу нового дистрибутива ключевой информации пользователю.

9. Технические мероприятия

9.1. Технические мероприятия по обслуживанию Компонентов ЗВС АГМ организуются Администратором ЗВС АГМ.

9.2. В случае возникновения производственной необходимости проведения ремонтных и планово-профилактических работ доступ к ЗВС АГМ или ее отдельным Компонентам может быть закрыт.

9.3. О проведении плановых работ (кроме аварийных и иных форс-мажорных ситуациях) Администратор ЗВС АГМ уведомляет всех Участников с использованием сервиса «Защищенная электронная почта» ЗВС АГМ не менее чем за 24 часа до намеченного срока начала работ.

10. Порядок разрешения конфликтных ситуаций

10.1. Возникновение конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения

Участниками электронных документов и/или получением доступа к информационным системам или ресурсам других Участников.

10.2. Разрешение конфликтных ситуаций осуществляется путем взаимодействия Пользователей Участников, у которых возникли претензии.

10.3. В случае необходимости, для разрешения конфликтных ситуаций может быть привлечен Администратор ЗВС АГМ.

11. Внесение изменений (дополнений) в Регламент

11.1. Внесение изменений (дополнений) в Регламент осуществляется Владельцем ЗВС АГМ по предложениям от Администратора ЗВС АГМ и Участников ЗВС АГМ в одностороннем порядке.

11.2. Все приложения, изменения и дополнения к Регламенту являются его составной и неотъемлемой частью.

Приложение № 1
к Регламенту

(Оформляется на бланке
Организации-заявителя)

Отдел информационно-технического
обеспечения и защиты информации
администрации города Мурманска

Наименование и адрес организации –
Администратора ЗВС АГМ

Заявление
о подключении к защищенной виртуальной сети администрации города Мурманска

_____
(Дата)

В соответствии с _____
(основание для подключения)
прошу рассмотреть запрос на подключение _____
(наименование организации)
к защищенной виртуальной сети администрации города Мурманска ViPNet № 4195.

Перечень информационных систем/информационных ресурсов, к которым необходим доступ:
_____
(наименование информационных систем/информационных ресурсов)

Предполагаемое число подключаемых Абонентских пунктов: _____
(указывается при подключении рабочих станций посредством Компонента ViPNet Client)

Лицо, ответственное за подключение, контактный телефон и адрес электронной почты:

_____
(ФИО, должность, контактные данные)

_____ _____ _____
(Должность руководителя) (Подпись) (Инициалы/Фамилия)

М.П.

СОГЛАСОВАНО
Начальник отдела информационно-технического обеспечения и защиты информации администрации города Мурманска

_____ _____
(Подпись) (Инициалы/Фамилия)

М.П.

Приложение № 2
к Регламенту

(Оформляется на бланке
Организации-заявителя)

Отдел информационно-технического
обеспечения и защиты информации
администрации города Мурманска

Наименование и адрес организации –
Администратора ЗВС АГМ

Заявление
на регистрацию пользователя защищенной виртуальной сети
администрации города Мурманска

_____
(Дата)

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность, фамилия, имя, отчество)

действующего на основании _____
(организационно-распорядительный документ)

просит изготовить дистрибутив ключевой информации на своего уполномоченного представителя – Пользователя защищенной виртуальной сети администрации города Мурманска (далее – ЗВС АГМ) в соответствии с указанными в настоящем заявлении данными:

Наименование юридического лица	Указывается краткое наименование юридического лица Участника
ФИО уполномоченного лица	Указываются фамилия, имя, отчество уполномоченного лица
Место нахождения (адрес установки абонентского пункта)	Указывается место установки программного обеспечения
Направления связи для организации защищенного обмена информацией	Указывается перечень Участников ЗВС АГМ, которых необходимо включить в направления связи (если требуется)
Перечень информационных систем или ресурсов, к которым необходим доступ	Указывается перечень информационных систем или ресурсов, к которым предполагается получить доступ посредством ЗВС АГМ (если требуется)

(*Все поля заполняются максимально полно. Фамилия, имя, отчество впечатываются в именительном падеже, все поля заполняются исключительно в печатном виде. Заполнение «от руки» недопустимо)

Администратором безопасности в _____
(наименование организации)

за эксплуатацию сетевого узла ЗВС АГМ назначен _____
(Ф.И.О., занимаемая должность, телефон)

Руководитель организации _____ _____
(Подпись) (Инициалы/Фамилия)

М.П.

С требованиями приказа ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» ознакомлен.

Уполномоченное лицо _____ _____
(Подпись) (Инициалы/Фамилия)

Администратор безопасности _____ _____
(Подпись) (Инициалы/Фамилия)

СОГЛАСОВАНО
Начальник отдела информационно-технического обеспечения и защиты информации администрации города Мурманска _____ _____
(Подпись) (Инициалы/Фамилия)

М.П.

Приложение № 3
к Регламенту

(Оформляется на бланке Организации-заявителя)

Наименование и адрес организации – Администратора ЗВС АГМ

Доверенность
на получение средств криптографической защиты информации

Дата выдачи _____
(дата прописью)

_____
(наименование организации)

в лице _____,
(должность и ФИО руководителя - полностью)

действующего на основании _____,

настоящей доверенностью уполномочивает _____

_____,
(должность и ФИО – полностью)

паспорт серия _____№ _____ выдан «___» _____года

_____, представлять интересы
(кем выдан)

_____ и получить
(ФИО и должность уполномоченного лица)

средства криптографической защиты информации, а также дистрибутивы ключевой информации защищенной виртуальной сети ViPNet администрации города Мурманска (ЗВС АГМ) и выполнить все необходимые действия, связанные с исполнением настоящего поручения.

Администратором безопасности в _____
(наименование организации)

за эксплуатацию сетевого узла ЗВС АГМ назначен _____
(Ф.И.О., занимаемая должность, телефон)

_____.

Доверенность действительна до «___» _____ 20___ года и дана без права передоверия.

Подпись лица, получившего доверенность _____.
(Подпись)

Руководитель _____ _____
(Подпись) (Инициалы/Фамилия)

М.П.

Приложение № 4
к Регламенту

(Оформляется на бланке Организации-заявителя)

Наименование и адрес организации – Администратора ЗВС АГМ

Заявление
на повторное формирование дистрибутива ключевой информации абонентского пункта защищенной виртуальной сети администрации города Мурманска

_____
(Дата)

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность, фамилия, имя, отчество)

действующего на основании _____,
(организационно-распорядительный документ)

просит осуществить повторное формирование и выдачу дистрибутива ключевой информации абонентского пункта защищенной виртуальной сети администрации города Мурманска

_____
(наименование абонентского пункта /идентификатор пользователя абонентского пункта)

в связи с

_____
(причина повторного формирования)

Руководитель организации _____ _____
(Подпись) (Инициалы/Фамилия)

М.П.

С требованиями приказа ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» ознакомлен.

Уполномоченное лицо _____ _____
(Подпись) (Инициалы/Фамилия)

Администратор безопасности _____ _____
(Подпись) (Инициалы/Фамилия)

Приложение № 5
к Регламенту

(Оформляется на бланке
Организации-заявителя)

Отдел информационно-технического
обеспечения и защиты информации
администрации города Мурманска

Наименование и адрес организации –
Администратора ЗВС АГМ

Заявление
на изменение направлений связи абонентского пункта защищенной виртуальной сети
администрации города Мурманска

_____
(Дата)

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность, фамилия, имя, отчество)

действующего на основании _____,
(организационно-распорядительный документ)

просит внести изменения в направления связи абонентского(их) пункта(ов) защищенной виртуальной сети администрации города Мурманска (далее – ЗВС АГМ), в соответствии с указанными в настоящем заявлении данными:

Наименование юридического лица	Указывается краткое наименование юридического лица Участника
Наименование абонентского пункта Участника	Указывается наименование абонентского пункта и идентификатор сетевого узла ЗВС АГМ
Направления связи для организации защищенного обмена информацией	Указывается перечень Участников ЗВС АГМ, которых необходимо включить в направления связи (если требуется)
Перечень информационных систем или ресурсов, к которым необходим доступ	Указывается перечень информационных систем или ресурсов, к которым необходимо получить доступ посредством ЗВС АГМ (если требуется)
Операция с направлениями связи	Указывается необходимая операция: Добавить/Удалить

(*Все поля заполняются максимально полно. Фамилия, имя, отчество впечатываются в именительном падеже, все поля заполняются исключительно в печатном виде. Заполнение «от руки» недопустимо)

Руководитель организации _____ _____
(Подпись) (Инициалы/Фамилия)

М.П.

С требованиями приказа ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» ознакомлен.

Уполномоченное лицо _____ _____
(Подпись) (Инициалы/Фамилия)

Администратор безопасности _____ _____
(Подпись) (Инициалы/Фамилия)

СОГЛАСОВАНО
Начальник отдела информационно-технического обеспечения и защиты информации администрации города Мурманска _____ _____
(Подпись) (Инициалы/Фамилия)

М.П.

Приложение № 6
к Регламенту

(Оформляется на бланке
Организации-заявителя)

Отдел информационно-технического
обеспечения и защиты информации
администрации города Мурманска

Наименование и адрес организации –
Администратора ЗВС АГМ

Уведомление
о компрометации криптографических ключей

Настоящим уведомляю о компрометации криптографических ключей абонентского пункта защищенной виртуальной сети администрации города Мурманска (далее – ЗВС АГМ) ViPNet № 4195

_____,
(наименование абонентского пункта /идентификатор пользователя абонентского пункта)

сформированных на уполномоченного представителя _____,
(ФИО пользователя)

использовавшихся в _____.
(наименование организации)

Компрометация криптографических ключей произошла по причине (подчеркнуть):

– увольнения сотрудников, имевших доступ к ключевой информации;
– доступа к компьютеру пользователя неуполномоченных лиц;
– обнаружения на компьютере пользователя вредоносного кода (вирусов, троянских программ и т.д.);
– иных причин: _____

Данные ключи прошу считать скомпрометированными и выведенными из действия с _____ час. _____ мин. по московскому времени «_____» _____ 20___ г.

Руководитель организации _____ _____
(Подпись) (Инициалы/Фамилия)

«____» _____ 20__ г.

М.П.

Примечание:
Дата и время вывода криптографических ключей из действия, указываемые в настоящем Уведомлении, не могут быть ранее даты и времени получения данного Уведомления Администратором ЗВС АГМ или получения сообщения о компрометации Администратором ЗВС АГМ по телефону или иным путем.
В случае если Администратор безопасности/Пользователь Участника, формирующий настоящее Уведомление, ранее сообщил Администратору ЗВС АГМ о компрометации данных криптографических ключей по телефону, то в настоящем Уведомлении время и дата вывода криптографических ключей из действия определяется временем и датой соответствующего сообщения по телефону.

Приложение № 7
к Регламенту

(Оформляется на бланке
Организации-заявителя)

Отдел информационно-технического
обеспечения и защиты информации
администрации города Мурманска

Наименование и адрес организации –
Администратора ЗВС АГМ

Об отключении от защищенной сети
администрации города Мурманска

Прошу произвести отключение _____
(наименование организации)
от защищенной виртуальной сети администрации города Мурманска ViPNet № 4195, а также считать все криптографические ключи абонентских пунктов скомпрометированными и выведенными из действия с _____ час. _____ мин. по московскому времени «_____» _____ 20___ г.

_____	_____	_____
(Должность руководителя)	(Подпись)	(Инициалы/Фамилия)

«____» _____ 20__ г.

СОГЛАСОВАНО
Начальник отдела информационно-технического обеспечения и защиты информации администрации города Мурманска

_____	_____
(Подпись)	(Инициалы/Фамилия)

М.П.

Приложение № 8
к Регламенту

Соглашение №_____
об установлении межсетевого взаимодействия

г. Мурманск «__» _____20__ г.

_____, в лице _____,
(наименование Организации, включая организационно-правовую форму) (должность, ФИО)

действующего на основании _____, в дальнейшем именуемое «_____»,
(сокращенное наименование Организации)

с одной стороны, и_____
(наименование Организации, включая организационно-правовую форму)

в лице _____, действующего на основании_____,
(должность, ФИО)

именуемое в дальнейшем «_____», с другой стороны,
(сокращенное наименование Организации)

совместно именуемые «Стороны», заключили настоящее соглашение об установлении межсетевого взаимодействия (далее – Соглашение) о нижеследующем:

1. Предмет Соглашения

1.1. Стороны договорились об установлении межсетевого взаимодействия и доверия между сетевыми узлами ViPNet-сети «_____» (далее – ViPNet №_____) и сетевыми узлами ViPNet-сети «_____» (далее – ViPNet №_____). Межсетевое взаимодействие обеспечивает создание защищенной и доверенной среды обработки информации ограниченного доступа между разрешенными сетевыми узлами ViPNet-сетей Сторон.

1.2. Отношения между Сторонами регулируются следующими нормативными документами:

– Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– приказом ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

– приказом ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

– иными нормативными правовыми актами, регулирующими деятельность Сторон.

1.3. Стороны признают, что используемые ими при межсетевом взаимодействии средства криптографической защиты информации (далее - СКЗИ) ViPNet, реализующие функции шифрования, сертифицированы Федеральной службой безопасности Российской Федерации и достаточны для обеспечения конфиденциальности при обработке информации ограниченного доступа Сторон.

1.4. С целью исполнения условий настоящего Соглашения Стороны самостоятельно приобретают и устанавливают на свои аппаратные средства программное (программно-аппаратное) обеспечение ViPNet, а также обеспечивают его работоспособность.

1.5. Взаимодействие Сторон осуществляется на безвозмездной основе.

2. Права и обязанности Сторон

2.1. При организации межсетевого взаимодействия «_____» принимает на себя следующие права и обязанности:

2.1.1. Обеспечивает поддержание в работоспособном состоянии программных и программно-аппаратных комплексов ViPNet №_____ в границах своей зоны ответственности.

2.1.2. Обеспечивает организацию взаимосвязи с сетевыми узлами ViPNet №_____ в соответствии с разделом 3 настоящего Соглашения.

2.1.3. Определяет уполномоченных лиц, ответственных за взаимодействие в рамках настоящего Соглашения (далее – уполномоченные лица), и сообщает «_____» об определении таких уполномоченных лиц с указанием их контактных данных.

2.1.4. Организовывает режим функционирования СКЗИ ViPNet таким образом, чтобы исключить возможность их использования, использования ключей шифрования лицами, не имеющими допуска к работе с ними.

2.2. При организации межсетевого взаимодействия «_____» принимает на себя следующие права и обязанности:

2.2.1. Обеспечивает поддержание в работоспособном состоянии программных и программно-аппаратных комплексов ViPNet № ____ в границах своей зоны ответственности.

2.2.2. Обеспечивает организацию взаимосвязи с сетевыми узлами ViPNet № _____ в соответствии с разделом 3 настоящего Соглашения.

2.2.3. Определяет уполномоченных лиц, ответственных за взаимодействие в рамках настоящего Соглашения, и сообщает «_____» об определении таких уполномоченных лиц с указанием их контактных данных.

2.2.4. Организовывает режим функционирования СКЗИ ViPNet таким образом, чтобы исключить возможность их использования, использования ключей шифрования лицами, не имеющими допуска к работе с ними.

2.3. Стороны обеспечивают контроль за проведением процедуры обмена данными экспорта между центрами управления сетью программного обеспечения (далее – ПО) ViPNet Administrator защищенных сетей.

2.4. Привлечение Сторонами третьих лиц к монтажу (установке) и настройке сетевых узлов защищенных сетей ViPNet разрешается в случае наличия у них лицензии ФСБ России, выданной в соответствии с Положением о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утвержденным постановлением Правительства Российской Федерации от 16.04.2012 № 313, и разрешающей следующий вид деятельности: «Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств».

2.5. В целях обеспечения безопасности обработки и конфиденциальности информации ограниченного доступа Стороны обязаны:

– не разглашать и не передавать третьим лицам (обеспечить конфиденциальность) информацию, связанную с осуществлением информационного обмена в рамках межсетевого взаимодействия, за исключением случаев, предусмотренных действующим законодательством;

– обеспечить информационную безопасность и техническую защиту информации каждого используемого рабочего места и сетевого узла защищенных сетей ViPNet в межсетевом взаимодействии в соответствии с законодательством Российской Федерации;

– соблюдать требования технической и эксплуатационной документации на сетевые узлы ViPNet;

– незамедлительно информировать ответственных лиц Сторон в случае выявления инцидента информационной безопасности, который может угрожать безопасности информации в инфраструктуре Сторон.

3. Организация межсетевого взаимодействия

3.1. Ответственными лицами Сторон для организации межсетевого взаимодействия являются Администраторы защищенных сетей. На начальном этапе организуется межсетевое взаимодействие только между сетевыми узлами Администраторов Сторон через шлюзовые ViPNet-Координаторы в соответствии с технической документацией на СКЗИ ViPNet.

3.2. По завершении процедуры организации межсетевого взаимодействия между ViPNet № _____ и ViPNet № _____ подписывается протокол установления межсетевого взаимодействия (приложение № 1).

3.3. Смена межсетевых мастер-ключей, изменение состава сетевых узлов, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чем Администраторы защищенных сетей уведомляют друг друга с помощью ПО ViPNet или направлением письма на адрес электронной почты уполномоченных лиц Сторон (приложение № 2) с указанием производимых изменений.

4. Проведение профилактических мероприятий

4.1. Проведение профилактических мероприятий по поддержанию работоспособности программных и программно-аппаратных комплексов ViPNet в границах своей зоны ответственности Стороны осуществляют при соблюдении следующего условия – о сроках проведения профилактических мероприятий другая Сторона должна быть оповещена заблаговременно, не позднее чем за три рабочих дня до дня проведения профилактических мероприятий.

4.2. В случае возникновения необходимости проведения технических работ, следствием которых может быть временное прекращение работоспособности программных и программно-аппаратных комплексов ViPNet, Сторона-инициатор должна уведомить другую Сторону по электронной почте или по телефону.

5. Ответственность Сторон

Стороны несут ответственность за обеспечение безопасности информации, передаваемой по средствам программных и программно-аппаратных комплексов ViPNet в границах своей зоны ответственности согласно законодательству Российской Федерации.

6. Сроки действия Соглашения

6.1. Настоящее Соглашение вступает в силу с даты его подписания и действует бессрочно.

6.2. В случае нарушения одной из Сторон обязательств, предусмотренных данным Соглашением, другая Сторона вправе в одностороннем порядке расторгнуть настоящее Соглашение, уведомив об этом другую Сторону в письменном виде за один день. Во всех иных случаях каждая из Сторон вправе в одностороннем порядке расторгнуть настоящее Соглашение, уведомив об этом в письменном виде другую Сторону за один месяц.

7. Форс-мажор

7.1. При возникновении обстоятельств, которые делают полностью или частично невозможным выполнение настоящего Соглашения одной из

Сторон, таких как стихийные бедствия, военные действия и другие обстоятельства непреодолимой силы, не зависящие от Сторон, сроки исполнения обязательств продлеваются на время, в течение которого действуют эти обстоятельства.

7.2. Сторона, подвергшаяся действию форс-мажорных обстоятельств, обязуется уведомить письменно другую Сторону в течение трех рабочих дней с предоставлением документов, подтверждающих наличие данных обстоятельств.

7.3. Если обстоятельства непреодолимой силы действуют более одного месяца, Соглашение может быть досрочно расторгнуто в одностороннем порядке путем заключения дополнительного соглашения.

8. Дополнительные условия

8.1. В случае возникновения споров и разногласий Стороны прилагают все усилия, чтобы устранить их путём переговоров.

8.2. При возникновении обстоятельств, которые не позволяют обеспечить межсетевое взаимодействие между ViPNet № ____ и ViPNet № _____ Стороны прилагают совместные усилия по устранению этих обстоятельств.

8.3. Любые изменения и дополнения к Соглашению действительны, если они совершены в письменной форме и подписаны надлежащим образом уполномоченными на то представителями Сторон.

8.4. В случае изменения наименования, адреса места нахождения или других реквизитов одной из Сторон Сторона письменно извещает об этом другую Сторону в течение трех рабочих дней со дня такого изменения.

8.5. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

8.6. К настоящему Соглашению прилагаются в качестве неотъемлемой части следующие приложения:

8.6.1. Приложение № 1. Форма протокола установления межсетевого взаимодействия.

8.6.2. Приложение № 2. Список уполномоченных лиц.

9. Адреса и реквизиты Сторон

_____/_____/ _____/_____/

МП МП

Приложение № 1
к Соглашению от _____ №_____

Протокол
установления межсетевого взаимодействия

_____ «___» _____ 20__г.

1. Межсетевое взаимодействие устанавливается между сетями:

Номер сети	Наименование организации

2. Целью установления межсетевого взаимодействия является межведомственное защищенное информационное взаимодействие ViPNet №_____ и ViPNet №_____.

3. Процедуру установления межсетевого взаимодействия осуществляли:

Номер сети	Должность	ФИО

4. Передача начального и ответного экспорта между сетями ViPNet №____ и ViPNet № ____ осуществлялась через специалиста, уполномоченного на данные действия.

5. Для установления межсетевого взаимодействия использовался индивидуальный симметричный межсетевой мастер-ключ, созданный в сети ViPNet № ____.

6. Для установления межсетевого взаимодействия были назначены маршрутизаторы для организации шлюза:

- в сети ViPNet № _____ – «_____»;
- в сети ViPNet № _____ – «_____».

7. При установлении межсетевого взаимодействия в части создания связей между сетевыми узлами были произведены импорты справочников из сети ViPNet №____ и сети ViPNet № _____.

8. Стороны обязуются производить изменения в настройках и структуре защищенных сетей, которые могут привести к нарушению межсетевого взаимодействия, только после предварительного согласования.

Администратор ViPNet №____ Администратор ViPNet №_____

_____ / _____ _____ / _____

Приложение № 2
к Соглашению от _____ №_____

Список уполномоченных лиц «_____»
(от организации участника информационного взаимодействия)

№ п/п	Ф.И.О.	Должность	Контактный телефон	Роль	Название сетевого узла
1					
2					
3					

Список уполномоченных лиц «_____»
(от организации участника информационного взаимодействия)

№ п/п	Ф.И.О.	Должность	Контактный телефон	Роль	Название сетевого узла
1					
2					
3					